Strong Secrecy for Erasure Wiretap Channels

Ananda T. Suresh*, Arunkumar Subramanian†, Andrew Thangaraj*, Matthieu Bloch† and Steven McLaughlin†
* Department of Electrical Engineering, Indian Institute of Technology, Madras
Email: andrew@iitm.ac.in
† School of Electrical and Computer Engineering, Georgia Institute of Technology, USA and GT-CNRS UMI 2958, France
Email: arunkumar@gatech.edu, matthieu.bloch@ece.gatech.edu, swm@ece.gatech.edu

***Abstract*—We show that duals of certain low-density parity-check (LDPC) codes, when used in a standard coset coding scheme, provide strong secrecy over the binary erasure wiretap channel (BEWC). This result hinges on a stopping set analysis of ensembles of LDPC codes with block length n and girth $\geq 2k$, for some $k \geq 2$. We show that if the minimum left degree of the ensemble is $l_{\min}$, the expected probability of block error is $\mathcal{O}(\frac{1}{n^{\lceil l_{\min} k/2 \rceil - k}})$ when the erasure probability $\epsilon < \epsilon_{\text{ef}}$, where ϵ_{ef} depends on the degree distribution of the ensemble. As long as $l_{\min} > 2$ and $k > 2$, the dual of this LDPC code provides strong secrecy over a BEWC of erasure probability greater than $1 - \epsilon_{\text{ef}}$.**

I. Introduction

The information-theoretic limits of secure communications over public channels were first investigated by Shannon [1]; given a message M and its corresponding cryptogram X^n of length n, a message is communicated with *perfect secrecy* if $\mathbb{I}(\mathsf{M}; \mathsf{X}^n) = 0$. Shannon proved the disappointing result that perfect secrecy requires a secret key K with entropy $\mathbb{H}(\mathsf{K}) \geq \mathbb{H}(\mathsf{M})$. In this setting, Wyner subsequently proposed an alternative model for secure communication called a *wiretap channel* [2], in which all communications occur over noisy channels and the eavesdropper observes a degraded version Z^n of the signal received by the legitimate receiver. Wyner introduced the notion of *weak secrecy*, which requires the leaked information *rate* $\frac{1}{n}\mathbb{I}(\mathsf{M}; \mathsf{Z}^n)$ to vanish as $n \to \infty$, and established the *weak secrecy capacity*, that is the maximum secure communication rate achievable over a wiretap channel under this condition. Maurer and Wolf later highlighted the shortcomings of weak secrecy for cryptographic purposes, and suggested to replace it with the notion of *strong secrecy*, by which the absolute information $\mathbb{I}(\mathsf{M}; \mathsf{Z}^n)$ should vanish as $n \to \infty$. Surprisingly, this stronger secrecy requirement does not reduce secrecy capacity [3], [4].

Despite the surge of recent results investigating wiretap channels, the design of coding schemes with provable secrecy rate has not attracted much attention. Some efforts in coding for wiretap channels include [5]–[9].

In this work, we revisit the LDPC-based coset coding scheme of [7] for the binary erasure wiretap channel. We first show that the dual of randomly generated LDPC codes can achieve strong secrecy provided the probability of block error of the LDPC codes decays faster than $\frac{1}{n}$ with the block length n in a binary erasure channel. Then, we show that for certain small-cycle-free LDPC ensembles, the probability of block error under iterative decoding decays as $\mathcal{O}(\frac{1}{n^2})$. We obtain this result by analyzing the stopping sets of LDPC ensembles. Stopping sets [10], [11] determine whether iterative decoding of LDPC codes under erasures will succeed or not. Asymptotic enumeration of stopping sets has been done by several authors (see [12]–[15] and references thereof). We follow the approach in [12], where asymptotics of the average block error probability of LDPC codes were derived.

Ensembles of LDPC codes with better than $\frac{1}{n}$ average block error probability are known from prior studies which use expander-based ideas and stopping set expurgation [16], [17]. Expander-based ideas typically require minimum bit node degree of five or above resulting in a decrease in thresholds. Expurgation of stopping sets is usually more difficult to achieve than expurgation of short cycles in random constructions. In our approach, we consider ensembles with finite girth. Restricting the girth results in $\mathcal{O}(\frac{1}{n^2})$ expected block error probability in irregular ensembles with minimum girth 4 and minimum bit node degree 3. This enables high erasure thresholds and efficient construction methods.

In this work, the code construction for strong secrecy is fundamentally different from Maurer and Wolf's procedure to obtain strong secrecy from weak secrecy [3]. Maurer and Wolf's method relies on the equivalence of key-generation with one-way communication and coding for the wiretap channel, while our code construction yields a forward error-control scheme directly. Nevertheless, the constraint imposed in our code construction limits the achievable secrecy rate.

The rest of the paper is organized as follows. In Section II, we briefly review the coset coding scheme for the binary erasure wiretap channel and establish the connection between strong secrecy and the decay of probability of block error with code length. In Section III, we show that the probability of block error for ensembles without short cycles decays fast enough to guarantee strong secrecy.

II. Secrecy Coding for the Binary Erasure Wiretap Channel

The wiretap channel considered in this work, denoted by BEWC(ϵ), is illustrated in Fig. 1. The channel between the legitimate parties is noiseless while the eavesdropper's channel is a binary erasure channel with erasure probability ϵ (denoted BEC(ϵ)). The secrecy capacity of this wiretap channel is $C_s = \epsilon$ [2].

The "coset coding" scheme to communicate secretly over this channel, proposed in [6], is the following. Prior to

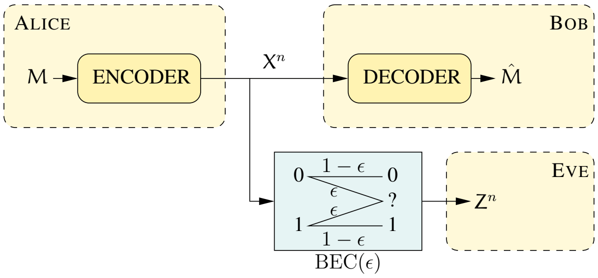

Fig. 1. Binary erasure wiretap channel.

transmission, Alice and Bob agree on a $(n, n-k)$ code C with parity check matrix $\mathbf{H}$. The coset of C with syndrome s^k is denoted by $C(\mathsf{s}^k) = \{\mathsf{x}^n \in \{0,1\}^n : \mathsf{s}^k = \mathbf{H}^T \mathsf{x}^n\}$. To transmit a message M of k bits, Alice transmits a codeword X^n chosen uniformly at random in $C(\mathsf{M})$. Bob decodes his received codeword X^n by forming the syndrome $\mathbf{H}^T \mathsf{X}^n$.

The following theorem due to Ozarow and Wyner connects the equivocation of the eavesdropper to algebraic properties of the generator matrix.

Theorem 1 ([6]). *Let C be a $(n, n-k)$ code with generator matrix $\mathbf{G} = [g_1, \dots, g_n]$, where g_i represents the i-th column of $\mathbf{G}$. Let z^n be an observation of the eavesdropper with μ unerased position given by $\{i : z_i \neq ?\} = \{i_1, \dots, i_\mu\}$. Let $\mathbf{G}_\mu = [g_{i_1} \dots g_{i_\mu}]$. Then, $\mathbb{H}(\mathsf{M}|\mathsf{z}^n) = k$ iff $\mathbf{G}_\mu$ has full rank.*

Based on Theorem 1, we can now connect the rate of convergence of $\mathbb{I}(\mathsf{M}; \mathsf{Z}^n)$ to the probability that a submatrix of $\mathbf{G}$ has full rank.

Lemma 1. *Let G_μ be the submatrix of $\mathbf{G}$ corresponding to the unerased positions in Z^n. Let p_{nf} be the probability that G_μ is not full rank. Then, a coset coding scheme operates with strong secrecy if the probability p_{nf} is such that $p_{nf} = \mathcal{O}(\frac{1}{n^\alpha})$ for some $\alpha > 1$.*

Proof: We can lower bound $\mathbb{H}(\mathsf{M}|\mathsf{Z}^n)$ as

$$\begin{aligned} \mathbb{H}(\mathsf{M}|\mathsf{Z}^n) &\geq \mathbb{H}(\mathsf{M}|\mathsf{Z}^n, \operatorname{rank}(G_\mu)) \\ &\geq \mathbb{H}(\mathsf{M}|\mathsf{Z}^n, G_\mu \text{ is full rank})\, \mathbb{P}[G_\mu \text{ is full rank}] \\ &= k(1 - p_{nf}) = k - R_s n p_{nf} \end{aligned}$$

If $p_{nf} = \mathcal{O}(\frac{1}{n^\alpha})$, then $\mathbb{I}(\mathsf{M}; \mathsf{Z}^n) = k - \mathbb{H}(\mathsf{M}|\mathsf{Z}^n) \leq \mathcal{O}(\frac{1}{n^{\alpha-1}})$, which can be made arbitrary small for n sufficiently large and $\alpha > 1$. ■

Let $C^n(\lambda, \rho)$ be an LDPC ensemble with n variable nodes, left edge degree distributions $\lambda(x) = \sum_{i \geq 1} \lambda_i x^{i-1}$ and right node degree distribution $\rho(x) = \sum_{i \geq 1} \rho_i x^{i-1}$ [15, §3.4] with possibly some expurgations. The degree distributions $\lambda(x), \rho(x)$ are from an edge perspective, that is λ_i is the fraction of edges connected to a variable node of degree i and ρ_j is similarly defined.

Let $P_e^{(n)}(\epsilon)$ denote the probability of block error for codes from $C^n(\lambda, \rho)$ over BEC(ϵ) under iterative decoding. An important interpretation of $P_e^{(n)}(\epsilon)$ is the following: for a parity-check matrix H with degree distribution (λ, ρ), $1 - P_e^{(n)}(\epsilon)$ is a lower bound on the probability that erased columns of H (over a BEC(ϵ)) form a full-rank submatrix. Using this interpretation and results from [7], we have the following immediate corollary of Lemma 1.

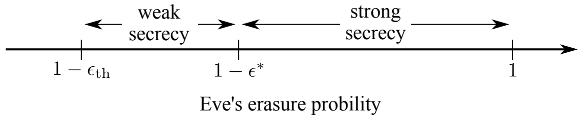

Fig. 2. Weak and strong secrecy regions using duals of LDPC codes

Corollary 1. *If there exists $\epsilon^* > 0$ such that $P_e^{(n)}(\epsilon) = \mathcal{O}(\frac{1}{n^\alpha})$, ($\alpha > 1$) for $\epsilon < \epsilon^*$, then the dual of a code from $C^n(\lambda, \rho)$ used in a coset coding scheme provides strong secrecy over a* BEWC(ϵ) *for $\epsilon > 1 - \epsilon^*$.*

It is immediately clear that we will have $\epsilon^* \leq \epsilon_{\text{th}}$, where ϵ_{th} is the erasure threshold for the ensemble over LDPC codes [15]. As noted in [7], when $\epsilon \leq \epsilon_{\text{th}}$ we have weak secrecy. In view of this, we will have *guaranteed* weak and strong secrecy regions as illustrated in Fig. 2 by doing "coset coding" using duals of LDPC codes. We know that degree distributions can be optimized so that $1 - \epsilon_{\text{th}}$ is very close to the code rate. Since LDPC codes achieve capacity over a BEC, our coding scheme will achieve weak secrecy very close to the secrecy rate and strong secrecy slightly away from the secrecy rate. In the next section, we will show that ϵ^* exists for some restricted ensembles of LDPC codes.

III. THE LDPC ENSEMBLE WITHOUT SHORT CYCLES

In this section, we study the sub-ensemble of Tanner graphs [15] whose girth is at least $2k$ for some integer $k \geq 2$ which does not change with the block length n. We denote the ensemble of all Tanner graphs by $\mathcal{G}(n, \lambda, \rho)$ and the sub-ensemble of girth $\geq g$ graphs by $\mathcal{G}_g(n, \lambda, \rho)$. We associate i *sockets* to each node of degree i. An edge in a Tanner graph is an unordered pair containing one bit node socket and one check node socket. A Tanner graph with $|E|$ edges has $|E|$ sockets on each side. Therefore, the size of the ensemble equal to the number of permutation of the check node sockets, which is $|E|!$. First we show that the size of our sub-ensemble is not negligible compared to the size of the original ensemble as $n \to \infty$.

Lemma 2 ([18, Corollary 4]). *Let n, g be even positive integers and $d \geq 3$ be an integer. As n grows, let $(d-1)^{2g-1} = o(n)$. Then, the number of (labeled) d-regular bipartite graphs on n vertices with girth greater than g is*

$$\frac{(nd/2)!}{(d!)^n} \exp\left(-\sum_{s=1}^{g/2} \frac{(d-1)^{2s}}{2s} + o(1) \right)$$

as $n \to \infty$.

Note that the number of d-regular bipartite graphs on n vertices is $(nd/2)!/(d!)^n$. The following corollary is then immediate.

Corollary 2. *Let g, n be positive even numbers and let $d \geq 3$ be an integer. Let d, g remain constant as $n \to \infty$. Then, the fraction of (d, d) regular bipartite graphs that have girth greater than g is*

$$\exp\left(-\sum_{s=1}^{g/2} \frac{(d-1)^{2s}}{2s} + o(1)\right)$$

as $n \to \infty$. In particular, this fraction is bounded away from zero for large n.

Lemma 3. *Let a (λ, ρ) irregular Tanner graph ensemble be such that $\max\{\deg(\lambda), \deg(\rho)\} > 2$ and the coefficients of the degree distribution polynomials are rational. Let $g > 0$ be an integer that remains constant with block length n. There exists an increasing sequence (n_k) of positive integers such that the fraction of graphs of girth $> g$ in $\mathcal{G}(n_k, \lambda, \rho)$ is bounded away from zero as $k \to \infty$.*

Proof: Let d be the least common multiple of all the vertex degrees in the graph. Clearly, $d > 2$ and it is a function of only λ and ρ. Let a be the smallest positive integer such that

$$\tfrac{a\tilde{\lambda}_i}{d}, \qquad \tfrac{a\tilde{\rho}_j}{d} \in \mathbb{N}$$

where $\tilde{\lambda}_i$ is the fraction of variable nodes of degree i and $\tilde{\rho}_j$ is the fraction of check nodes of degree j [15, §3.4]. Consider the Tanner graph ensemble with $n_k = ak$ variable nodes. We can group d/i of the degree i variable nodes to get one variable node of degree d. If we do this for all the variable node degrees, we will have a left regular Tanner graph with left degree d. Similarly, we can repeat this process for the check nodes to get a (d, d) regular Tanner graph. Note that in this node grouping process, we preserve the number of edges since the ensemble allows the possibility of multiple edges. The girth of the resultant regular graph is not more than that of the original graph. It can also be noted that there is a one-one correspondence between the graphs in the (λ, ρ) ensemble and those in the (d, d) ensemble. By lemma 2, the fraction of graphs with girth $> g$ in the (d, d) ensemble, say μ, is non-zero if k is large enough. So, the fraction of graphs in the (λ, ρ) ensemble with girth $> g$ is at least μ. This proves the lemma. ■

Remark 1. *Let X be a graph dependent positive number. Let $\mathbb{E}X$ represent the expectation of X over $\mathcal{G}(n, \lambda, \rho)$. Let $\mathbb{E}_1 X$ be the expectation over $\mathcal{G}_g(n, \lambda, \rho)$ and $\mathbb{E}_2 X$ be the expectation over $\mathcal{G}(n, \lambda, \rho) \setminus \mathcal{G}_g(n, \lambda, \rho)$. We have*

$$\mathbb{E}X = q_n \mathbb{E}_1 X + (1 - q_n)\mathbb{E}_2 X$$

where $q_n \triangleq |\mathcal{G}_g(n, \lambda, \rho)|/|\mathcal{G}(n, \lambda, \rho)|$. By lemma 3, there exists a $p > 0$ such that for large n, we have $q_n \geq p$. Therefore,

$$\mathbb{E}X \geq p\mathbb{E}_1 X$$
$$\mathbb{E}_1 X \leq \frac{1}{p}\mathbb{E}X$$

This inequality is used to upper bound $\mathbb{E}_1 X$ when it is easier to find an upper bound to $\mathbb{E}X$.

A. Stopping sets and stopping number

For the sake of clarity and completeness, we restate some of the definitions that were originally stated in [12]. Given a Tanner graph G, let U be any subset of variable nodes in G. Let the (check node) neighbours of U be denoted by $N(U)$. U is called a *stopping set* if the degree of all the check nodes in the induced subgraph $G[U \cup N(U)]$ is at least two. The *stopping number* of a Tanner graph is defined as the size of its smallest stopping set. For a given Tanner graph, its stopping number is denoted by s^* and the set of all stopping sets is denoted by $\mathbb{S}$. The *stopping ratio* is defined as the ratio of the stopping number to the block length.

The *average stopping set distribution* is defined as

$$E(s) = \mathbb{E}(|\{S \in \mathbb{S} : |S| = s\}|)$$

where the average is taken over all the Tanner graphs in $\mathcal{G}(n, \rho, \lambda)$. For any rational $\alpha \in [0, 1]$, it is assumed that there exists a sequence (n_k) of strictly increasing block lengths such that $E(\alpha n_k) > 0$ for all n_k. We can then define the *normalized stopping set distribution* as

$$\gamma(\alpha) = \lim_{k \to \infty} \frac{1}{n_k} \log E(\alpha n_k)$$

It was shown that $\gamma(\alpha)$ is continuous over the set of rationals and hence, it can be extended to a continuous function over $[0, 1]$. The *critical exponent stopping ratio* of a Tanner graph ensemble is defined as

$$\alpha^* = \inf\{\alpha > 0 : \gamma(\alpha) \geq 0\}$$

B. Block error probability of short-cycle-free ensembles

In this section, we prove a key result about the average block error probability of short-cycle-free LDPC ensembles, which is central to our claim that the duals of these codes provide strong secrecy. Let $P_B^{\mathrm{IT}}(C, \epsilon)$ be the probability of block error when the code C is transmitted over $\mathrm{BEC}(\epsilon)$ and iteratively decoded. We define [12]

$$\epsilon_{\mathrm{ef}} \triangleq \sup\left\{\epsilon : \max_{\alpha \in [0, \epsilon]} \left(\gamma(\alpha) + (1 - \alpha)h(\tfrac{\epsilon - \alpha}{1 - \alpha}) - h(\epsilon)\right) \leq 0\right\}$$

where $h(x)$ is the binary entropy function calculated using natural logarithms. Note that $\gamma(\alpha)$, and ϵ_{ef} are calculated over the entire ensemble $\mathcal{G}(n, \lambda, \rho)$ instead of the girth-restricted ensemble. Instead of calculating $P_B^{\mathrm{IT}}(C, \epsilon)$ directly, we take averages of this quantity over an ensemble of codes and show that the average block error probability over the ensemble $\mathcal{G}_{2k}(n, \lambda, \rho)$ decays as fast as we want it to for $\epsilon < \epsilon_{\mathrm{ef}}$.

Theorem 2. *For $\mathcal{G}_{2k}(n, \lambda, \rho)$, with minimum variable node degree $l_{\min}$, maximum variable node degree $l_{\max}$ and maximum check node degree $r_{\max} > 2$ we have*

$$\mathbb{E}_1(P_B^{\mathrm{IT}}(C, \epsilon)) = \mathcal{O}\left(\frac{1}{n^{\lceil \frac{l_{\min}}{2} k \rceil - k}}\right)$$

and in the limits of small ϵ and large n

$$\mathbb{E}_1(P_B^{\mathrm{IT}}(C, \epsilon)) = \mathcal{O}\left(\frac{\epsilon^k}{n^{\lceil \frac{l_{\min}}{2} k \rceil - k}}\right)$$

Proof: Let V_e be the set of variable nodes corresponding to the random erasures in the LDPC codeword. The iterative decoding fails iff V_e contains a stopping set. So,

$$P_B^{\mathrm{IT}}(C,\epsilon) = \mathbb{P}(\exists S \in \mathbb{S} : S \subset V_e)$$

For any $\delta_1, \delta_2 > 0$, we bound $P_B^{\mathrm{IT}}(C,\epsilon)$ using union bound as

$$\begin{aligned} P_B^{\mathrm{IT}}(C,\epsilon) \leq & \sum_{i=k}^{\delta_1 n-1} \left|\{S \in \mathbb{S} : |S| = i\}\right| \epsilon^i \\ & + \mathbb{P}(\exists S \in \mathbb{S} : S \subset V_e, \delta_1 n \leq |S| \leq (\epsilon+\delta_2)n) \\ & + \mathbb{P}(\exists S \in \mathbb{S} : S \subset V_e, (\epsilon+\delta_2)n \leq |S| \leq n) \end{aligned}$$

Using an argument almost identical to the one used in [12, Theorem 16], we can show that the expectations of the second and the third terms go to zero exponentially as $n \to \infty$ if $\epsilon < \epsilon_{\mathrm{ef}}$. Now,

$$\begin{aligned} & \mathbb{E}_1\left(\sum_{i=k}^{\delta_1 n-1} \left|\{S \in \mathbb{S} : |S| = i\}\right| \epsilon^i\right) \\ & \quad = \sum_{i=k}^{\delta_1 n-1} \mathbb{E}_1\left(\left|\{S \in \mathbb{S} : |S| = i\}\right|\right) \epsilon^i \\ & \quad \leq \frac{1}{p} \sum_{i=k}^{\delta_1 n-1} \mathbb{E}\left(\left|\{S \in \mathbb{S} : |S| = i\}\right|\right) \epsilon^i \end{aligned}$$

A stopping set of i variable nodes can have nodes of different degrees. Let $\mathcal{S}_i$ denote the set of all non-negative integer solutions to the equation $i_{l_{\min}} + i_{l_{\min}+1} + \cdots + i_{l_{\max}} = i$. We can write

$$\begin{aligned} & \mathbb{E}\left(\left|\{S \in \mathbb{S} : |S| = i\}\right|\right) \epsilon^i \\ & \quad = \epsilon^i \sum_{\{i_s\} \in \mathcal{S}_i} \tbinom{n\tilde{\lambda}_{l_{\min}}}{i_{l_{\min}}} \tbinom{n\tilde{\lambda}_{l_{\min}+1}}{i_{l_{\min}+1}} \cdots \tbinom{n\tilde{\lambda}_{l_{\max}}}{i_{l_{\max}}} \frac{A}{\binom{|E|}{\sum s i_s}} \\ & \quad \leq \epsilon^i \binom{n}{i} \sum_{\{i_s\} \in \mathcal{S}_i} \frac{A}{\binom{|E|}{\sum s i_s}} \end{aligned}$$

Here, A is the number of ways to connect the selected i variable nodes to form a stopping set. This number is independent of n as long as i is just a small fraction of it. We also note that if we increase the degree of all the check nodes in the graph, A can only increase. Therefore, we may upper bound A by the number of ways to form a stopping set assuming each check node has the maximum possible degree, $r_{\max}$. The latter number is equal to coef $\left(\left((1+x)^{r_{\max}} - r_{\max}x\right)^m, x^{\sum s i_s}\right)$ by elementary combinatorics. We have,

$$\begin{aligned} A & \leq \operatorname{coef}\left(\left((1+x)^{r_{\max}} - r_{\max}x\right)^m, x^{\sum s i_s}\right) \\ & \leq \binom{m + \lfloor \frac{\sum s i_s}{2} \rfloor - \lceil \frac{\sum s i_s}{r_{\max}} \rceil}{\lfloor \frac{\sum s i_s}{2} \rfloor} (2r_{\max} - 3)^{\sum s i_s} \end{aligned}$$

where the last inequality follows from [12, Lemma 18]. If we denote $\sum s i_s$ by w, we have $il_{\min} \leq w \leq il_{\max}$. So,

$$\begin{aligned} & \mathbb{E}\left(\left|\{S \in \mathbb{S} : |S| = i\}\right|\right) \epsilon^i \\ & \quad \leq \epsilon^i \binom{n}{i} \sum_{\{i_s\} \in \mathcal{S}_i} \binom{m + \lfloor \frac{w}{2} \rfloor - \lceil \frac{w}{r_{\max}} \rceil}{\lfloor \frac{w}{2} \rfloor} \frac{(2r_{\max}-3)^w}{\binom{|E|}{w}} \\ & \quad \leq \epsilon^i \binom{n}{i} (2r_{\max}-3)^{il_{\max}} \sum_{\{i_s\} \in \mathcal{S}_i} \binom{m + \frac{il_{\max}}{2}}{\lfloor \frac{w}{2} \rfloor} \frac{1}{\binom{|E|}{w}} \\ & \quad \leq \epsilon^i \binom{n}{i} (2r_{\max}-3)^{il_{\max}} \sum_{\{i_s\} \in \mathcal{S}_i} \frac{\left(m + \frac{il_{\max}}{2}\right)^{\lfloor \frac{w}{2} \rfloor} w!}{\lfloor \frac{w}{2} \rfloor! \left(|E| - il_{\max}\right)^w} \end{aligned}$$

If we denote the summand by $f(w)$, we have

$$\tfrac{f(2r+1)}{f(2r)} = \tfrac{2r+1}{|E|-il_{\max}} \leq \tfrac{il_{\max}}{|E|-il_{\max}} \leq \tfrac{\delta n l_{\max}}{|E|-\delta_1 n l_{\max}} \leq 1$$

if we choose δ_1 small enough. Also,

$$\tfrac{f(2r+2)}{f(2r+1)} = 2\tfrac{m+\frac{il_{\max}}{2}}{|E|-il_{\max}} \leq 2\tfrac{m+\frac{\delta_1 n l_{\max}}{2}}{|E|-\delta_1 n l_{\max}}$$

Since $r_{\max} > 2$ we have $|E| > 2m$. Again, if we choose δ_1 small enough, we will have $f(2r+2)/f(2r+1) \leq 1$. So, $f(w)$ is a non-increasing function and $w \geq il_{\min}$. We now have

$$\begin{aligned} & \mathbb{E}\left(\left|\{S \in \mathbb{S} : |S| = i\}\right|\right) \epsilon^i \\ & \quad \leq \epsilon^i \tbinom{n}{i} (2r_{\max}-3)^{il_{\max}} \\ & \qquad \times \sum_{\{i_s\} \in \mathcal{S}_i} \frac{\left(m + \frac{il_{\max}}{2}\right)^{\lfloor \frac{il_{\min}}{2} \rfloor} (il_{\min})!}{\lfloor \frac{il_{\min}}{2} \rfloor! \left(|E| - il_{\max}\right)^{il_{\min}}} \\ & \quad \leq \epsilon^i \tbinom{n}{i} (2r_{\max}-3)^{il_{\max}} (i+1)^{r_{\max}} \\ & \qquad \times \frac{\left(m + \frac{\delta_1 n l_{\max}}{2}\right)^{\lfloor \frac{il_{\min}}{2} \rfloor} (il_{\min})!}{\lfloor \frac{il_{\min}}{2} \rfloor! \left(|E| - \delta_1 n l_{\max}\right)^{il_{\min}}} \\ & \quad \leq \epsilon^i \tbinom{n}{i} (2r_{\max}-3)^{il_{\max}} \frac{(i+1)^{r_{\max}}}{n^{\lceil \frac{il_{\min}}{2} \rceil}} \\ & \qquad \times \frac{\left(r_0 + \frac{\delta_1 r_{\max}}{2}\right)^{\lfloor \frac{il_{\min}}{2} \rfloor} (il_{\min})!}{\lfloor \frac{il_{\min}}{2} \rfloor! \left(r_1 - \delta_1 r_{\max}\right)^{il_{\min}}} \\ & \quad \triangleq \epsilon^i J_i \end{aligned}$$

Here, $r_0 = m/n$ and $r_1 = |E|/n$ depend only on ρ and λ. If i remains a constant as $n \to \infty$, we have

$$J_i = \Theta\left(\frac{1}{n^{\lceil \frac{il_{\min}}{2} \rceil - i}}\right) \tag{1}$$

Also,

$$\begin{aligned} \frac{J_{i+2}}{J_i} & = \frac{\binom{n}{i+2}}{\binom{n}{i}} (2r_{\max}-3)^{2l_{\max}} \frac{\left(r_0 + \frac{\delta_1 l_{\max}}{2}\right)^{l_{\min}}}{\left(r_1 - \delta_1 l_{\max}\right)^{2l_{\min}}} \\ & \qquad \times \left(\tfrac{i+3}{i+1}\right)^{r_{\max}} \frac{(il_{\min} + 2l_{\min})! \lfloor \frac{il_{\min}}{2} \rfloor!}{(il_{\min})! \left(\lfloor \frac{il_{\min}}{2} \rfloor + l_{\min}\right)! n^{l_{\min}}} \\ & \leq \frac{(n-i-1)(n-i)}{(i+1)(i+2)} (2r_{\max}-3)^{2l_{\max}} \left(\tfrac{i+3}{i+1}\right)^{r_{\max}} \\ & \qquad \times \frac{\left(r_0 + \frac{\delta_1 l_{\max}}{2}\right)^{l_{\min}}}{\left(r_1 - \delta_1 l_{\max}\right)^{2l_{\min}}} \; \frac{(il_{\min} + 2l_{\min})^{2l_{\min}}}{\left(\lfloor \frac{il_{\min}}{2} \rfloor + 1\right)^{l_{\min}} n^{l_{\min}}} \end{aligned}$$

Using $\frac{i+3}{i+1} \leq 2$, $il_{\min} + 2l_{\min} \leq 3il_{\min}$, $\lfloor x \rfloor + 1 \geq x$,

$$\begin{aligned}\frac{J_{i+2}}{J_i} \leq{}& \frac{n^2}{i^2}(2r_{\max} - 3)^{2l_{\max}} 2^{r_{\max}} \frac{(r_0 + \frac{\delta_1 l_{\max}}{2})^{l_{\min}}}{(r_1 - \delta_1 l_{\max})^{2l_{\min}}} \\ &\times \frac{(3il_{\min})^{2l_{\min}}}{\left(\frac{il_{\min}}{2}\right)^{l_{\min}} n^{l_{\min}}}\end{aligned}$$

Choosing $\delta_3 \in (0,1)$ such that $r_1 - \delta_3 l_{\max} > 0$ and $\delta_1 < \delta_3$,

$$\begin{aligned}\frac{J_{i+2}}{J_i} &\leq (2r_{\max} - 3)^{2l_{\max}} 2^{r_{\max}} \\ &\quad \times \frac{(r_0 + \frac{\delta_3 l_{\max}}{2})^{l_{\min}} (3l_{\min})^{2l_{\min}}}{(r_1 - \delta_3 l_{\max})^{2l_{\min}} \left(\frac{l_{\min}}{2}\right)^{l_{\min}}} \left(\frac{i}{n}\right)^{l_{\min}-2} \\ &= B\left(\frac{i}{n}\right)^{l_{\min}-2} \quad \leq \quad B\delta_1^{l_{\min}-2}\end{aligned}$$

where B depends only on λ and ρ.

$$\begin{aligned}\mathbb{E}_1 &\left(\sum_{i=k}^{\delta_1 n - 1} \left| \{ S \in \mathbb{S} : |S| = i \} \right| \epsilon^i \right) \leq \frac{1}{p} \sum_{i=k}^{\delta_1 n - 1} \epsilon^i J_i \\ &\leq \frac{1}{p}\epsilon^k \sum_{i=k}^{\delta_1 n - 1} J_i \\ &= \frac{1}{p}\epsilon^k \left[\Theta\left(\frac{1}{n^{\lceil \frac{l_{\min}}{2} k \rceil - k}} \right) + \Theta\left(\frac{1}{n^{\lceil \frac{l_{\min}}{2}(k+1) \rceil - k - 1}} \right) \right] \\ &\quad \times \sum_{i=0}^{\delta_1 n/2} \left(B\delta_1^{l_{\min}-2} \right)^i\end{aligned}$$

If δ_1 is small enough, then the summation in the above equation is bounded by a decreasing geometric sum. So,

$$\begin{aligned}\mathbb{E}_1 \left(\sum_{i=k}^{\delta_1 n - 1} \left| \{ S \in \mathbb{S} : |S| = i \} \right| \epsilon^i \right) &= \mathcal{O}\left(\frac{\epsilon^k}{n^{\lceil \frac{l_{\min}}{2} k \rceil - k}} \right) \\ \Rightarrow \mathbb{E}_1 \left(P_B^{\mathrm{IT}}(C, \epsilon) \right) &= \mathcal{O}\left(\frac{\epsilon^k}{n^{\lceil \frac{l_{\min}}{2} k \rceil - k}} \right) \quad (2)\end{aligned}$$

as $\epsilon \to 0$ and $n \to \infty$. ■

From the above theorem, the average block error probability in our ensemble decays faster than $\frac{1}{n^2}$ for $l_{\min} > 2$ and $k > 3$. This correpsonds to LDPC ensembles with a minimum bit node degree of at least 3 and girth at least 4. By corollary 1, the duals of these LDPC codes achieve strong secrecy over a BEWC of erasure probability $1 - \epsilon_{\mathrm{ef}}$.

The (3, 6) regular LDPC ensemble has $\epsilon_{\mathrm{th}} = 0.429$, $\epsilon_{\mathrm{ef}} = 0.366$ and rate $1/2$. When duals of codes in this ensemble are used on $\mathrm{BEWC}(\epsilon)$, a secret communication rate of 0.5 is achieved with weak secrecy when $\epsilon \in (0.571, 0.634)$ and with strong secrecy when $\epsilon > 0.634$. Our numerical calculations indicate that some of the degree distributions that are optimized for very high ϵ_{th} have $\epsilon_{\mathrm{ef}} < 0.366$.

IV. Conclusion and future directions

In this work, we have shown that duals of LDPC codes with girth greater than 4 and minimum left degree at least 3 achieve strong secrecy on the binary erasure wiretap channel. LDPC ensembles with degree 2 nodes play an important role in achieving capacity on the binary erasure channel. Further study is required on the relationship between these LDPC codes and strong secrecy. Another research possibility involves optimizing the degree distributions to find LDPC ensembles with a very high ϵ_{ef} for a given rate.

References

[1] C. E. Shannon, “Communication Theory of Secrecy Systems,” *Bell System Technical Journal*, vol. 28, pp. 656–715, 1948.

[2] A. D. Wyner, “The Wire-Tap Channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, October 1975.

[3] U. M. Maurer and S. Wolf, “Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free,” in *Advances in Cryptology - Eurocrypt 2000*, Lecture Notes in Computer Science. B. Preneel, 2000, p. 351.

[4] I. Csiszár, “Almost Independence and Secrecy Capacity,” *Problems of Information Transmission*, vol. 32, no. 1, pp. 40–47, January-March 1996.

[5] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, “Generalized Privacy Amplification,” *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, November 1995.

[6] L. H. Ozarow and A. D. Wyner, “Wire Tap Channel II,” *AT&T Bell Laboratories Technical Journal*, vol. 63, no. 10, pp. 2135–2157, December 1984.

[7] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, “Applications of LDPC Codes to the Wiretap Channels,” *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[8] R. Liu, Y. Liang, H. V. Poor, and P. Spasojević, “Secure Nested Codes for Type II Wiretap Channels,” in *Proceedings of IEEE Information Theory Workshop*, Lake Tahoe, California, USA, September 2007, pp. 337–342.

[9] G. Cohen and G. Zemor, “Syndrome-Coding for the Wiretap Channel Revisited,” in *Proc. IEEE Information Theory Workshop*, Chengdu, China, October 2006, pp. 33–36.

[10] C. Di, D. Proietti, I. Telatar, T. Richardson, and R. Urbanke, “Finite-length analysis of low-density parity-check codes on the binary erasure channel,” *Information Theory, IEEE Transactions on*, vol. 48, no. 6, pp. 1570 –1579, jun 2002.

[11] T. Richardson and R. Urbanke, “The capacity of low-density parity-check codes under message-passing decoding,” *Information Theory, IEEE Transactions on*, vol. 47, no. 2, pp. 599 –618, feb 2001.

[12] A. Orlitsky, K. Viswanathan, and J. Zhang, “Stopping set distribution of LDPC code ensembles,” *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 929 –953, march 2005.

[13] O. Milenkovic, E. Soljanin, and P. Whiting, “Asymptotic spectra of trapping sets in regular and irregular ldpc code ensembles,” *Information Theory, IEEE Transactions on*, vol. 53, no. 1, pp. 39 –55, jan. 2007.

[14] D. Burshtein and G. Miller, “Asymptotic enumeration methods for analyzing ldpc codes,” *Information Theory, IEEE Transactions on*, vol. 50, no. 6, pp. 1115 – 1131, june 2004.

[15] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge University Press, 2008.

[16] S. Korada and R. Urbanke, “Exchange of limits: Why iterative decoding works,” in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, july 2008, pp. 285 –289.

[17] A. Amraoui, A. Montanari, T. Richardson, and R. Urbanke, “Finite-length scaling for iteratively decoded ldpc ensembles,” *Information Theory, IEEE Transactions on*, vol. 55, no. 2, pp. 473 –498, feb. 2009.

[18] B. D. McKay, N. C. Wormald, and B. Wysocka, “Short cycles in random regular graphs,” *Electr. J. Comb.*, vol. 11, no. 1, 2004.